EXHIBIT A

1001.1—1001.3: Document Security, Inquiries and Freedom of Information Act Requests

Policy 1001.1: Confidentiality and Security

Confidentiality

All Hotline investigations and inclusive documents require strict adherence to confidentiality standards.

- Hotline cases should not be discussed except by the IAD, OSIG-authorized personnel or others included on a "need-to-know" basis.
- Hotline Investigative/Complaint Report sheets shall not be shared, except among individuals conducting the investigation.
- The State Inspector General or designee is authorized to distribute or release Hotline reports.
- All documents, working papers, notes and reports dealing with an investigation shall be marked "Confidential State Fraud, Waste and Abuse Hotline Document."
- Interviews and investigation information should not be shared, discussed or given to anyone who does not have a legitimate need for access.
- Strict confidentiality must be maintained throughout the entire Hotline investigation.

Physical Security

All Hotline documents must be maintained in a secured environment. All custodians of Hotline documents, such as IADs and OSIG staff shall maintain all information supporting Hotline investigations in a secured location. All such information, documentation, etc. is the property of OSIG and shall be identified as such. OSIG may request that supporting information and documentation accompany formal reports.

Written Communications

- Hotline reports and other sensitive documents should be transmitted electronically between OSIG and state agencies that possess digital encryption capabilities, or agreed upon password protected documents.
- Commonwealth inter-agency mail should never be used to send Hotline information/documents.
- Fax communications and correspondence via the United State Postal Service (USPS) are permitted under certain circumstances only after prior discussion with OSIG.